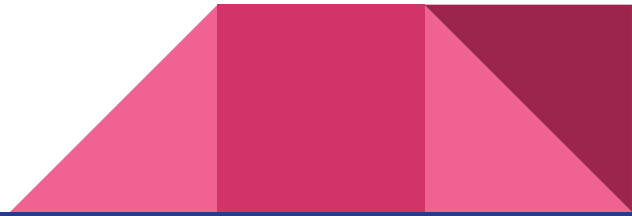
Autentizace na ZČU

Ing. Pavel Jindra, CIV

SecFest 2019,Plzeň

Autentizace

- Prokázání elektronické identity člověka
  - něco znám - heslo
  - něco mám - autentizační token
  - něco umím - vyřešit hádanku (otázky)
  - něco jsem - biometrické údaje
- Jednoduchá
  - pro každou službu se ověřuji znova
  - každá služba zná mé údaje
- Centrální
  - vždy se ověřuji k centrální službě
  - služba spoléhá na údaje z centrálního ověření
  - je možné řídit jaké os. údaje služba dostane



Autentizace na ZČU - hesla

- Hesla pro centrální autentizační systém Kerberos
  - Heslo ověřuje jednotná autorita KDC server
  - Po ověření (AS) je vydán lístek (TGT) kterým se uživatel ověřuje ke službám
    - omezená platnost - 8 hodin
  - Využití:
    - aplikační - přihlášení ssh (eryx), IMAP server,
    - windows - přihlášení, crossrealm
    - WEBové SSO - WebAuth, Shibboleth (federace eduID)
- Hesla pro “eduroam”
  - pouze pro přístup do eduroam
  - oddělená infrastruktura hesel
- Certifikáty na čipové kartě JIS
  - WEBové SSO, Magion

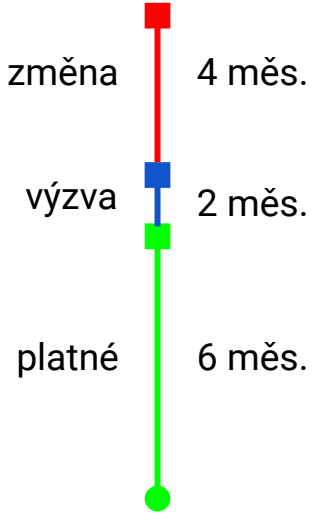
Hesla systému Kerberos

Současná politika hesla:

- délka 8 znaků, 2 skupiny znaků
- platnost 8 měsíců + 4 měsíce na změnu

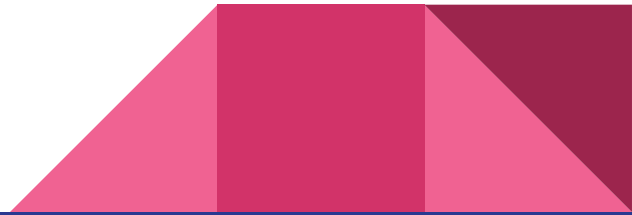
Nová politika hesla:

- délka 12 znaků, 2-3 skupiny znaků
- dostatečná entropie
- platnost 2 roky + 1 rok na změnu



Změny politiky hesel

- Kvalitnější heslo dovolí delší platnost
- Alespoň 1x za studium změnit heslo
  - aktualizace politiky hesel
  - uplatnění nových bezpečnějších šifer
  - zabránění “heslové archeologii”



Oddělené heslo pro “eduroam”

- Chrání pouze přístup do sítě
- “Válí” se na různých zařízení (mobil, notebook)
- Možné zneužití na špatně nakonfigurovaných systémech
  - falešný přístupový bod
- Politiky hesla:
  - platnost 6 měsíců - pravidelné prodlužování
  - délka 8 znaků, 2 skupiny
- Ochrana proti “heslové archeologii”
- Systémy sledující zneužití konta
- **Nemělo by být shodné s Orion heslem**

Závěr

- Volte silná a kvalitní hesla
- Heslo za žádných okolností nikomu nesdělujte
- Volte pro každou službu unikátní heslo
- Při podezření na únik heslo změňte
- Nepoužívejte ukládání hesel
- Ani velmi bezpečné heslo neodolá phishingu